Název práce: Logika a kryptografie

Autor: Bc. Vojtěch Wagner

Katedra: Katedra algebry

Vedoucí diplomové práce: prof. RNDr. Jan Krajíček, DrSc.

Abstrakt: Práce se zabývá studiem metod pro formalizaci kryptografických konstrukcí. Konkrétně metodou, která je založena na definování logické teorie T, která obsahuje řetězce, čísla a objekty třídy k - k-ární funkce. Povolíme jim určité operace a formulujeme axiomy, termy a formule. Budeme používat speciální typ termů - počítající term, který označuje počet prvků x v daném intervalu splňujících formuli $\varphi(x)$. Díky nim můžeme mluvit o pravděpodobnostech a používat další pojmy z teorie pravděpodobnosti. Práce nejprve popisuje detailně tuto teorii. Poté přináší formalizaci Goldreich-Levinovy věty. Cílem práce je předložit potřebné kryptografické pojmy a konstrukce v jazyce teorie T a následně dokázat větu pomocí objektů, pravidel a axiomů teorie T. Uvedené definice a principy jsou ilustrovány na příkladech. Cílem práce je ukázat, že takováto teorie je dostatečně silná, aby dokázala správnost a bezpečnost podobné kryptografické konstrukce.

Klíčová slova: kryptografie, ověřování protokolů, věta o správnosti, formální logická teorie, Goldreich-Levinova věta